REMARKS

Applicant respectfully requests reconsideration of this application, as amended, and consideration of the following remarks. Claims 1, 14, 17 and 19 have been amended. Claim 16 has been cancelled. Claims 1-15 and 17-20 remain pending. Claims 1-10, 12 and 14-20 stand rejected under 35 U.S.C. 102(e). Claims 11, 13 stand rejected under 35 U.S.C. 103(a).

Amendments

Amendments to the Claims

Applicant has amended the claims to more particularly point out what Applicant regards as the invention. [Summarize invention] No new matter has been added as a result of these amendments.

Rejections

Rejections under 35 U.S.C. §102(e) and 103(a)

Claims 1-10, 12 and 14-20 stand rejected under 35 U.S.C. 102(e) as being anticipated by Arnand (US Pat Pub 2002/0191792, now issued as US Pat 7,213,148). Claim 11 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Anand in view of Qi (US Pat Pub 2002/0184498). Claim 13 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Anand in view of Bradley (US Pat 6,711,633). Applicant respectfully traverses these rejections as set forth in more detail below.

The Anand reference discloses a hash processing system and method for reducing the number of clock cycles required to implement the SHA1 and MD5 hash algorithms by using a common hash memory having multiple storage areas each coupled to one of two or more hash channels. The system further provides implicit padding on-the-fly as data is read from the common hash memory. The system shares register and other circuit resources for MD5 and SHA1 hash circuits that are implemented in each hash channel, and uses pipelined, two-channel SHA1 and pipelined, single-channel MD5 hash architectures to reduce the effective time required to implement the SHA1 and MD5 algorithms.

Anand does not share components such as adders or compressors between the different hash circuits. Anand provides completely separate logic circuits to process each of the different types of hash functions (e.g., the circuit of Fig. 3 to perform a SHA-1 function, the circuit of Fig. 4 to perform an MD5 function) (col. 10, lines 6-10). Anand does share input and output registers for temporary storage of the data being processed by the different hash logic circuits. Sharing the input and output registers is not the same as sharing components within the actual hash function circuits 114, 116 because Anand uses each of the different hash function circuits ***in parallel*** and therefore ***cannot share*** hash functional components ***and maintain parallel function*** capability.

The Qi reference teaches an architecture (hardware implementation) for an authentication engine to increase the speed at which SHA1 multi-loop and/or multi-round authentication algorithms may be performed on data packets transmitted over a computer network. As described in this application, the invention has particular application to the variant of the SHA1 authentication algorithms specified by the IPSec cryptography standard. In accordance with the IPSec standard, the invention may be used in conjunction with data encryption/encryption architecture and protocols. However it is also suitable for use in conjunction with other non-IPSec cryptography algorithms, and for applications in which encryption/decryption is not conducted (in IPSec or not) and where it is purely authentication that is accelerated. Among other advantages, an authentication engine in accordance with the present invention provides improved performance with regard to the processing of short data packets.

The Bradley reference teaches a compressor circuit suitable for use in an arithmetic unit of a microprocessor includes a first stage, a second stage, a carry circuit, and a sum circuit. The first stage is configured to receive a set of four input signals. The first stage generates a first intermediate signal indicative of the XNOR of a first pair of the input signals and a second intermediate signal indicative of the XNOR of a second pair of the input signals. The second stage configured to receive at least a portion of the signals generated by the first stage. The second stage generates first and second control signals where the first control signal is indicative of the XNOR of the four input signals and the second control signal is the logical

complement of the first signal. The carry circuit is configured to receive at least one of the control signals and further configured to generate a carry bit based at least in part on the state of the received control signal. The sum circuit is configured to receive at least one of the control signals and further configured to generate a sum bit based at least in part on the state of the received control signal. At least one of the first stage, second stage, sum circuit, and carry circuit include at least one CMOS transmission gate comprised of an n-channel transistor and a p-channel transistor having their source/drain terminals connected in parallel, wherein the p-channel transistor gate is driven by the logical complement of the n-channel transistor gate. In one embodiment, the first stage, second stage, carry circuit, and sum circuit are comprised primarily of such transmission gates to the exclusion of conventional CMOS complementary passgate logic.

As to claims 1-15 and 17-20, none of the cited references whether considered alone or in combination teach or suggest a system method or apparatus where the hash modules share logic components (e.g., adders, compressors, etc.) that are selectable and used to perform the respective hash functions. Anand teaches completely separate adders for each hash function and does not disclose shared adders nor systems and methods of selecting the shared adders as claimed by Applicant. It would not be obvious to modify Anand as the separate hash circuits are typically functional blocks that are simply repeated to increase speed (e.g., parallel processing as described by Anand) and in a parallel processing circuit, the adders could not be shared and still maintain full parallel functionality. None of the other cited references correct this deficit in Anand.

Accordingly, Applicant respectfully submits that Applicant's invention as claimed in claims 1-15 and 17-20 is not rendered obvious by any of the cited references whether considered alone or in any combination, and respectfully request the withdrawal of the rejections under 35 U.S.C. §102(e) and 103(a).

SUMMARY

In view of the foregoing amendments and remarks, Applicant respectfully submits that the pending claims are in condition for allowance. Applicant respectfully requests reconsideration of the application and allowance of the pending claims.

If the Examiner determines the prompt allowance of these claims could be facilitated by a telephone conference, the Examiner is invited to contact George B. Leavell at (408) 749-6900, ext 6923.

Deposit Account Authorization

Authorization is hereby given to charge our Deposit Account No. 50-0805 (Ref SUNMP349) for any charges that may be due or credit our account for any overpayment. Furthermore, if an extension is required, then Applicant hereby requests such extension.

Respectfully submitted,

MARTINE PENILLA & GENCARELLA, LLP

Dated: June 28, 2007

George B. Leavell
Attorney for Applicant
Registration No. 45,436

710 Lakeway Drive, Suite 200
Sunnyvale, CA 94085
(408) 749-6900 ext 6923